

ISO/IEC 27018:2025, Informācijas drošība, kiberdrošība un privātuma aizsardzība: vadlīnijas personas datu (PII) aizsardzībai publiskajos mākoņos, kas darbojas kā PII apstrādātāji (3. izdevums, 2025-08)

Personas datu aizsardzība publiskajā mākonī

36 prasības. Šim standartam nav akreditēta sertifikāta. Redakcija 07/2026.

ISO/IEC 27018 nav pārvaldības sistēmas standarts, bet vadlīniju kopums ar paplašinātiem kontroles pasākumiem papildus ISO/IEC 27002:2022. Atsevišķa akreditēta sertifikāta par atbilstību ISO/IEC 27018 nav. Kontroles pasākumus iekļauj ISO/IEC 27001 sistēmas piemērojamības paziņojumā, un sertifikātu pēc tam izsniedz par atbilstību ISO/IEC 27001 ar atsauci uz ISO/IEC 27018. Standarts ir vērsts uz publiska mākoņpakalpojuma piegādātāju, kas apstrādā personas datus savu mākoņpakalpojuma klientu uzdevumā. Organizācija, kas mākoņpakalpojumus tikai izmanto, šo lomu neuzņemas, un tai ir lietderīgi novērtēt prasības attiecībā uz saviem piegādātājiem, nevis attiecībā uz sevi pašu. Leanshift gadījumā šis saraksts tāpēc galvenokārt ir piegādātāju novērtēšanas shēma. Katru punktu var uzdot piegādātājam kā jautājumu un nostiprināt datu apstrādes līgumā saskaņā ar GDPR 28. pantu. Šāda novērtējuma rezultāts ir iekšējs atbilstības ieraksts vai piegādātāja novērtējuma profils, nevis sertifikāts. Par numerāciju: nodaļas no A.2 līdz A.12 seko standarta A pielikuma privātuma principiem, bet punkti ar numuru, piemēram, A.11.6, ir tur uzskaitītie papildu kontroles pasākumi. Punkti ar numuru, piemēram, 8.10 vai 5.34, attiecas uz ISO/IEC 27002:2022 kontroles pasākumiem, kurus standarts precizē mākoņa videi. Punkti ar apzīmējumu (Grundsatz), kas nozīmē principu, ir atvasināti no pašas nodaļas principa tur, kur A pielikumā nav atsevišķa papildu kontroles pasākuma.

Uzņēmums	Datums	Aizpildīja

A.2 Piekrišana un izvēle2

A.2.1Mākoņpakalpojuma piegādātājs atbalsta mākoņpakalpojuma klientu datu subjektu tiesību izpildē, tostarp piekļuves, labošanas, dzēšanas un iebilduma tiesību izpildē. Atbildība un termiņi ir noteikti līgumā.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir datu apstrādes līgums saskaņā ar GDPR 28. pantu ar klauzulu par atbalstu datu subjektu tiesību izpildē, kopā ar tehniskajiem līdzekļiem pašā pakalpojumā: eksporta, labošanas un dzēšanas funkcijām vai dokumentētu atbalsta procedūru ar atbildes termiņu. Jautājums piegādātājam: kāda funkcija vai process ir pieejams, lai piekļuves vai dzēšanas pieprasījumu varētu izpildīt viena mēneša laikā?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.2 (Grundsatz)Mākoņpakalpojuma klientu personas datus apstrādā tikai saskaņā ar klienta dokumentētiem norādījumiem. Datu subjektu piekrišanas iegūšana paliek klienta kā pārziņa uzdevums, un piegādātājs to nepārņem.

Pēc kā to var atpazīt: Pierādījums ir norādījumu klauzula datu apstrādes līgumā un apliecinājums, ka piegādātājs datus sekundāri neizmanto, piemēram, pakalpojuma privātuma paziņojums un produkta dokumentācija. Jautājums piegādātājam: vai mūsu klientu dati kaut kādā veidā tiek apstrādāti ārpus mūsu norādījumiem, piemēram, produkta uzlabošanai vai modeļu apmācībai?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.3 Nolūka leģitimitāte un noteikšana2

A.3.1Nolūks, kādā piegādātājs apstrādā personas datus, aprobežojas ar nolīgta pakalpojuma sniegšanu un ir nosaukts līgumā. Apstrāde piegādātāja paša nolūkiem nenotiek.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir datu apstrādes līgums, kurā norādīts apstrādes priekšmets, raksturs, nolūks un ilgums, kā arī datu subjektu kategorijas saskaņā ar GDPR 28. panta 3. punktu. Jautājums piegādātājam: lūgums iesniegt līguma pielikumu, kurā apstrādes nolūks aprakstīts izsmeļoši. Mazam uzņēmumam pietiek ar piegādātāja standarta datu apstrādes pielikumu, ja tajā ir šī informācija.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.3.2

Piegādātājam uzticētos personas datus bez iepriekšējas skaidras piekrišanas neizmanto reklāmai, mārketingam vai citiem piegādātāja komerciāliem nolūkiem. Pakalpojuma sniegšana nav atkarīga no šādas piekrišanas.

Pēc kā to var atpazīt: Pierādījums ir skaidra līguma klauzula, kas izslēdz komerciālu sekundāro izmantošanu, kopā ar pakalpojuma lietošanas noteikumiem. Jautājums piegādātājam: rakstisks apliecinājums, ka klientu dati netiek izmantoti reklāmai, profilēšanai vai mākslīgā intelekta modeļu apmācībai. Ja šādas apņemšanās nav, pakalpojums personas datiem nav piemērots.

Atvērtā

Procesā

Izpildīta

Neattiecas

Pierādījums / pamatojums

A.4 Vākšanas ierobežošana

1

A.4 (Grunds)

Papildus datiem, ko klients ievada pakalpojumā, piegādātājs savām vajadzībām nevāc citus personas datus, tostarp telemetriju, lietošanas profilus vai satura analīzi. Darbības dati un metadati, kas tiek vākti, ir nosaukti un pamatoti.

Pēc kā to var atpazīt: Pierādījums ir saraksts ar datiem, kurus pakalpojums reģistrē papildus satura datiem (piekļuves žurnāli, telemetrija, diagnostikas dati), ar nolūku un glabāšanas termiņu, kā arī ekrānuzņēmums ar iestatījumu, kas izslēdz izvēles telemetriju. Jautājums piegādātājam: kādi lietošanas, telemetrijas un diagnostikas dati tiek vākti papildus, kādam nolūkam tie tiek izmantoti un vai vākšanu var izslēgt?

Atvērtā

Procesā

Izpildīta

Neattiecas

Pierādījums / pamatojums

A.5 Datu minimizēšana

2

A.5.1

Pagaidu faili, kas rodas personas datu apstrādes laikā, tostarp pagaidu krātuve, kešatmiņa vai atcelšanas žurnāli, tiek droši dzēsti noteiktā termiņā.

Pēc kā to var atpazīt: Pierādījums ir darbības vai dzēšanas procedūra ar noteiktu pagaidu datu glabāšanas termiņu, ko apstiprina sistēmas konfigurācija, piemēram, kešatmiņas TTL vai plānots tīrīšanas uzdevums ar tā izpildes žurnālu. Jautājums piegādātājam: pēc kāda termiņa tiek dzēsta kešatmiņa, pagaidu faili un starpstāvokļi, un kā to uzrauga?

Atvērtā

Procesā

Izpildīta

Neattiecas

Pierādījums / pamatojums

8.11

Visur, kur darbībai, testēšanai vai atbalstam nav nepieciešami reāli dati, personas dati ir maskēti, pseidonimizēti vai anonimizēti. Apstrādāto datu apjoms paliek ierobežots līdz tam, kas pakalpojumam patiešām nepieciešams.

Pēc kā to var atpazīt: Pierādījums ir noteikums par to, kurās vidēs drīkst būt reāli dati, kā arī ekrānuzņēmumi vai skripti par maskēšanu, ko izmanto testa un izstrādes sistēmās. Jautājums piegādātājam: vai atbalsta un izstrādes komandas strādā ar produkcijas vides datiem, un ja jā, ar kādiem aizsardzības pasākumiem? Mazam uzņēmumam pietiek ar noteikumu, ka testa sistēmas darbojas tikai ar ģenerētiem paraugdatiem.

Atvērtā

Procesā

Izpildīta

Neattiecas

Pierādījums / pamatojums

A.6 Izmantošanas, glabāšanas un izpaušanas ierobežošana

3

A.6.1

Ja piegādātājs saņem juridiski saistošu pieprasījumu izpaust personas datus, piemēram, no valsts iestādes, tas iepriekš informē mākoņpakalpojuma klientu, ciktāl to atļauj tiesību akti.

Pēc kā to var atpazīt: Pierādījums ir līgumiska paziņošanas klauzula un iekšējs process iestāžu pieprasījumiem ar nosauktu atbildīgo. Jautājums piegādātājam: vai pirms datu nodošanas tiek nosūtīts paziņojums, un vai tiek publicēts pārredzamības ziņojums par iestāžu pieprasījumiem? Aktuāls pārredzamības ziņojums ir spēcīgs pierādījums.

Atvērtā

Procesā

Izpildīta

Neattiecas

Pierādījums / pamatojums

A.6.2

Ja piegādātājs izpauž personas datus trešām personām, tas notikumu reģistrē izsekojami: kas datus saņēma, kad tas notika, kuri dati bija iesaistīti un uz kāda pamata izpaušana balstās.

Pēc kā to var atpazīt: Pierādījums ir izpaušanas reģistrs vai pieteikumu vēsture ar šiem laukiem, arī tad, ja tajā nav neviena ieraksta. Tukšs, bet uzturēts reģistrs ir pieņemams un ir praktiskais ceļš mazam uzņēmumam. Jautājums piegādātājam: vai tiek uzturēts datu izpaušanas reģistrs un vai no tā var saņemt izrakstus?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

Dokuments

8.10

Personas datus dzēš, tiklīdz beidzas līgumā noteiktais glabāšanas termiņš vai līgums, tostarp kopijas rezerves kopijās pēc to rotācijas cikla.

Pēc kā to var atpazīt: Pierādījums ir dzēšanas koncepcija ar glabāšanas termiņiem katrai datu kategorijai, rezerves kopiju glabāšanas termiņš un dzēšanas žurnāls vai dzēšanas apliecinājums. Jautājums piegādātājam: cik ilgi mūsu dati saglabājas rezerves kopijās pēc līguma izbeigšanas, un vai par to dzēšanu tiek izsniegts rakstisks apliecinājums?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7 Precizitāte un kvalitāte

2

A.7 (Grunds)

Piegādātājs pēc savas iniciatīvas negroza tam uzticētos personas datus. Labojumus un atjauninājumus veic vienīgi pēc mākoņpakalpojuma klienta norādījuma vai ar funkcijām, ko klients izmanto pats.

Pēc kā to var atpazīt: Pierādījums ir pakalpojuma rediģēšanas funkcijas kopā ar to izmaiņu vēsturi, kā arī norādījumu klauzula datu apstrādes līgumā. Jautājums piegādātājam: vai ierakstus var labot pašu spēkiem, un vai katra izmaiņa tiek žurnālēta izsekojami?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.13

Personas datu integritāte ir aizsargāta glabāšanā, pārraidē un atjaunošanā. Rezerves kopijas pastāv, un to atjaunojamība ir pārbaudīta.

Pēc kā to var atpazīt: Pierādījums ir rezerves kopiju konfigurācija, kontrolsummu vai integritātes mehānismi un vismaz viena dokumentēta atjaunošanas pārbaude gadā ar datumu un rezultātu. Jautājums piegādātājam: cik bieži tiek pārbaudīta atjaunošana un kāds atjaunošanas laiks ir noteikts pakalpojuma līmeņa līgumā?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8 Atklātība, pārredzamība un informēšana

2

A.8.1

Apakšuzņēmēju izmantošana personas datu apstrādē ir atklāta pirms līguma noslēgšanas. Par saraksta izmaiņām klientam paziņo savlaicīgi, lai klients varētu iebilst vai izbeigt līgumu.

Pēc kā to var atpazīt: Pierādījums ir aktuāls apakšapstrādātāju saraksts, publicēts vai darīts pieejams līgumiski, ar nosaukumu, valsti un apstrādes nolūku, kā arī paziņošanas noteikums saskaņā ar GDPR 28. panta 2. punktu. Jautājums piegādātājam: kur ir atrodams apakšapstrādātāju saraksts, cik ilgu laiku iepriekš tiek paziņots par izmaiņām un kā var iebilst?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

Dokuments

A.8 (Grunds)

Pirms līguma noslēgšanas piegādātājs dara pieejamu saprotamu informāciju par to, kā personas dati tiek apstrādāti, kādi aizsardzības pasākumi pastāv un kurās jurisdikcijās apstrāde notiek.

Pēc kā to var atpazīt: Pierādījums ir privātuma paziņojums, drošības apraksts, uzticības centra lapa un datu apstrādes līgums kopā ar tehniskajiem un organizatoriskajiem pasākumiem pielikumā. Jautājums piegādātājam: lūgums iesniegt aktuālo tehnisko un organizatorisko pasākumu sarakstu kā līguma pielikumu, nevis tikai mārketinga materiālu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.9 Personas līdzdalība un piekļuve

2

A.9 (Grundsaraksts) Pakalpojums dod mākoņpakalpojuma klientam tehniskus līdzekļus, lai datu subjektu piekļuves, labošanas un dzēšanas pieprasījumus izpildītu pašu spēkiem, piemēram, ar eksporta, meklēšanas un dzēšanas funkcijām.

Pēc kā to var atpazīt: Pierādījums ir eksporta un dzēšanas funkciju produkta dokumentācija, ko apstiprina iekšējs izmēģinājums: viens piekļuves pieprasījums tiek izpildīts no sākuma līdz beigām un tiek pierakstīts, cik ilgu laiku tas prasa. Jautājums piegādātājam: vai visus datus par vienu personu var atrast, eksportēt un dzēst bez piegādātāja atbalsta?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.34 Ja klients datu subjekta pieprasījumu nevar apstrādāt pats, piegādātājs sniedz atbalstu līgumā noteiktā termiņā. Pieprasījumus, ko datu subjekti nosūta tieši piegādātājam, nodod klientam, nevis atbild uz tiem pats piegādātājs.

Pēc kā to var atpazīt: Pierādījums ir attiecīgā klauzula datu apstrādes līgumā ar konkrētu atbildes termiņu, kā arī atbalsta pieteikumu vēsture kā reāls piemērs. Jautājums piegādātājam: kāds termiņš ir noteikts atbalstam datu subjektu tiesību izpildē un kādas ir tā izmaksas?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.10 Pārskatatbildība

4

A.10.1 Par personas datu aizsardzības pārkāpumiem mākoņpakalpojuma klientam ziņo bez nepamatotas kavēšanās, norādot apmēru, skartos datus, cēloni un veiktos pasākumus. Paziņošanas process ar atbildību un termiņiem ir noteikts.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir notikumu reaģēšanas plāns ar eskalācijas kādi, līgumā noteiktais paziņošanas termiņš (praksē darbojas 24 līdz 48 stundas, lai klients vēl paspētu ievērot 72 stundu termiņu saskaņā ar GDPR 33. pantu) un ieraksti par iepriekšējiem notikumiem vai par mācībām. Jautājums piegādātājam: kādā termiņā tiek ziņots par notikumu, pa kuru kanālu un kāda informācija tiek sniegta līdzī?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.10.2 Drošības politikas, darbības procedūras un ar tām saistītie ieraksti tiek saglabāti noteiktu laiku, lai apstrādi varētu rekonstruēt arī vēlāk.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir glabāšanas noteikums kopā ar politiku versiju vēsturi, piemēram, dokumentu reģistrā vai versiju kontroles sistēmā ar apstiprināšanas datumu. Jautājums piegādātājam: cik ilgi tiek glabātas politiku versijas un ar tām saistītie ieraksti, un vai audita gadījumā tiem var piekļūt?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.10.3 Pastāv noteikta kārtība personas datu atdošanai, pārņemšanai un iznīcināšanai līguma beigās, nosaucot formātus, termiņus un rīcību ar kopijām.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir izbeigšanas klauzula datu apstrādes līgumā un dzēšanas apliecinājums pēc līguma beigām. Jautājums piegādātājam: kādā formātā un kādā termiņā dati tiek atdoti, kad tiek iznīcinātas visas kopijas un vai par to tiek izsniegts rakstisks apliecinājums?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.35 Aizsardzības pasākumu rezultativitāte tiek regulāri neatkarīgi pārskatīta, piemēram, ar iekšējiem auditiem, ielaušanās testiem vai trešās puses apliecinājuma ziņojumiem. Rezultāti piemērotā veidā ir pieejami mākoņpakalpojuma klientam.

Pēc kā to var atpazīt: Pierādījums ir ISO/IEC 27001 sertifikāts ar piemērojamības paziņojumu, kurā iekļauti ISO/IEC 27018 kontroles pasākumi, vai SOC 2 ziņojums, kopā ar aktuāliem ielaušanās testu kopsavilkumiem. Jautājums piegādātājam: lūgums iesniegt sertifikātu, tā tvērumu un apliecinājumu, ka ISO/IEC 27018 ir atspoguļots piemērojamības paziņojumā. Svarīgi ir pārbaudīt, vai tvērums patiešām aptver izmantoto pakalpojumu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11 Informācijas drošība

13

A.11.1 Ikvienam, kam ir piekļuve personas datiem, ir saistošs konfidencialitātes pienākums neatkarīgi no tā, vai persona ir nodarbināta tieši vai piesaistīta no ārpusē.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir parakstītas konfidencialitātes vienošanās vai apliecinājumi, kas paliek spēkā arī pēc sadarbības beigām. Jautājums piegādātājam: vai visi darbinieki un pakalpojumu sniedzēji ar piekļuvi datiem ir rakstiski uzņēmušies konfidencialitātes pienākumu?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.2 Izdrukas un citas papīra kopijas ar personas datiem tiek veidotas tikai tur, kur tas ir absolūti nepieciešams. Pieļaujamo apjomu nosaka noteikums.

Pēc kā to var atpazīt: Pierādījums ir noteikums par rīcību ar izdrukām, kas datu centros parasti ir vispārējs drukāšanas aizliegums zonās ar klientu datiem. Jautājums piegādātājam: vai klientu dati vispār tiek drukāti, un ja jā, ar kādiem nosacījumiem?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.3 Atjaunošana no rezerves kopijām ir iepriekš atļauta, un žurnālā ir norādīta persona, kas atjaunošanu uzsākusi, un skartie dati.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir atjaunošanas žurnāls ar laika zīmogu, ierosinātāju un apjomu, ko rezerves kopiju rīks parasti veido automātiski. Jautājums piegādātājam: vai katra atjaunošana tiek žurnālā un vai audita gadījumā šie žurnāli ir apskatāmi?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.4 Datu nesēji ar personas datiem, kas atstāj telpas, ir aizsargāti pret neatļautu piekļuvi un nozaudēšanu, parasti ar šifrēšanu un transporta ierakstu.

Pēc kā to var atpazīt: Pierādījums ir šifrēšanas apliecinājums (pilna datu nesēja šifrēšana), transporta un nodošanas ieraksti un datu nesēju uzskaitē. Jautājums piegādātājam: vai datu nesēji ar klientu datiem kādreiz atstāj objektus, piemēram, rezerves kopiju vajadzībām, un kā tie ir aizsargāti pārvadāšanas laikā?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.5 Nešifrētu pārnēsājamu datu nesēju un ierīču izmantošana personas datiem ir aizliegta vai ierobežota līdz pamatotiem izņēmumiem ar dokumentētu apstiprinājumu.

Pēc kā to var atpazīt: Pierādījums ir noņemamo datu nesēju politika kopā ar tehnisku ieviešanu, piemēram, piespiedu ierīču šifrēšanu vai USB portiem, kas bloķēti ar ierīču pārvaldību. Jautājums piegādātājam: vai darbinieki var kopēt klientu datus uz nešifrētām ierīcēm un kas to tehniski novērš?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.6 Personas dati, kas tiek pārraidīti publiskajos tīklos, ir šifrēti. Izmantotie mehānismi atbilst pašreizējam tehnikas līmenim.

Pēc kā to var atpazīt: Pierādījums ir TLS konfigurācija (aktuāla protokola versija, bez novecojušiem šifru komplektiem) un ārējs konfigurācijas tests kā ziņojums. Praktiski mazam uzņēmumam: reizi gadā tiek veikta bezmaksas TLS skenēšana un rezultāts tiek saglabāts. Jautājums piegādātājam: kāda pārraides šifrēšana tiek piemērota un vai ir aktīva šifrēšana miera stāvoklī?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.7 Papīra ieraksti ar personas datiem tiek iznīcināti tā, ka to atjaunošana nav iespējama.

Pēc kā to var atpazīt: Pierādījums ir atbilstoša drošības līmeņa dokumentu smalcinātāji vai iznīcināšanas apliecinājumi no pakalpojuma sniedzēja, kas strādā saskaņā ar DIN 66399 vai līdzvērtīgu standartu. Jautājums piegādātājam: kā tiek iznīcināti papīra ieraksti par klientiem un vai iznīcināšanas apliecinājumi ir saglabāti?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.8 Lietotāju identifikatori ir piešķirti unikāli vienai personai, tos neizsniedz atkārtoti un nekopīgo. Koplietoti konti pastāv tikai pamatos izņēmumos un ar papildu izsekojamību.

Pēc kā to var atpazīt: Pierādījums ir lietotāju saraksts no identitātes sistēmas bez grupu kontiem, kopā ar noteikumu, ka administratīvais darbs notiek ar personisku kontu. Jautājums piegādātājam: vai ekspluatācijas personāls strādā ar personiskiem kontiem un vai daudzfaktoru autentifikācija ir obligāta?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.9 Piegādātājs jebkurā brīdī var norādīt, kurām personām vai lomām ir atļauta piekļuve personas datiem, un uztur šo pārskatu aktuālu.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir piekļuves tiesību pārskats pa lomām, ko apstiprina regulāra piekļuves pārskatīšana ar datumu un rezultātu. Mazam uzņēmumam pietiek ar reizi pusgadā veiktu lietotāju saraksta eksportu ar apstiprinājumu. Jautājums piegādātājam: cik darbinieku var piekļūt mūsu datiem un cik bieži tas tiek pārskatīts?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.10 Lietotāju konti tiek pārvaldīti visā to dzīves ciklā: izveide, izmaiņas un tūlītēja deaktivēšana, kad persona aiziet vai maina lomu.

Pēc kā to var atpazīt: Pierādījums ir darba uzsākšanas un izbeigšanas procedūra ar kontrolsarakstu, kā arī deaktivēto kontu žurnāli ar laika zīmogiem. Jautājums piegādātājam: kādā termiņā tiek atņemta piekļuve darbiniekiem, kas aiziet, un kā tas tiek pierādīts?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.11 Piegādātāja drošības un privātuma pienākumi ir noteikti līgumā, tostarp tehniskie un organizatoriskie pasākumi, klienta norādījumu saistošais spēks un klienta tiesības veikt auditu.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir parakstīts datu apstrādes līgums saskaņā ar GDPR 28. pantu ar pasākumu pielikumu un audita vai informācijas tiesībām. Jautājums piegādātājam: lūgums iesniegt parakstītu datu apstrādes līgumu kopā ar pielikumiem, nevis tikai atsauci uz vispārīgiem pakalpojuma noteikumiem.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.12 Apakšuzņēmējiem, kas apstrādā personas datus, ir vismaz tie paši pienākumi, kas pašam piegādātājam. To izvēli un pastāvīgu uzraudzību nosaka noteikts process.

Pēc kā to var atpazīt: Pierādījums ir pienākumu pārņemšana līgumos ar apakšuzņēmējiem (GDPR 28. panta 4. punkts) un piegādātāju novērtēšana ar datumu. Jautājums piegādātājam: kā tiek novērtēti apakšuzņēmēji un kādus pierādījumus no tiem pieprasa?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.13 Pirms krātuves vietas atkārtotas izmantošanas ir nodrošināts, ka iepriekšējo lietotāju dati nepaliek pieejami ne fiziskajos datu nesējos, ne virtualizētās vidēs.

Pēc kā to var atpazīt: Pierādījums ir attīrīšanas vai pārrakstīšanas procedūra, ko piemēro krātuves atbrīvošanas brīdī, ieraksti par datu nesēju iznīcināšanu un klientu nodalīšanu, kas aprakstīta arhitektūras dokumentā. Jautājums piegādātājam: kā tiek nodrošināts, ka atkārtoti izmantotā krātuvē nav citu klientu atlikušo datu?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.12 Privātuma atbilstība

3

A.12.1

Valstis, kurās personas dati tiek glabāti un apstrādāti, ir nosauktas un mākoņpakalpojuma klientam zināmas. Par glabāšanas vietu izmaiņām tiek paziņots.

Pēc kā to var atpazīt: Pierādījums ir piegādātāja pārskats par objektiem un reģioniem līgumā vai dokumentācijā, kā arī ekrānuzņēmums ar izmantotā pakalpojuma reģiona iestatījumu. Jautājums piegādātājam: kurās valstīs mūsu dati atrodas miera stāvoklī, no kurām valstīm tiem piekļūst, piemēram, atbalsta darbā, un vai reģionu var fiksēt?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.12.2

Personas datu nodošana uz trešām valstīm ir zināma, pamatota un nodrošināta ar atbilstošiem aizsardzības pasākumiem.

Pēc kā to var atpazīt: Pierādījums ir līguma standartklauzulas vai lēmums par aizsardzības līmeņa pietiekamību, ko apstiprina nodošanas ietekmes novērtējums, kas mazam uzņēmumam var būt īss: skartās datu kategorijas, saņēmēja valsts, risks, veiktie papildu pasākumi. Jautājums piegādātājam: uz kāda tiesiskā pamata dati tiek nodoti trešām valstīm un kādi papildu pasākumi tiek piemēroti?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.31

Juridiskās un līgumiskās prasības, kas attiecas uz personas datu apstrādi, ir apzinātas un tiek uzturētas aktuālas, mainoties tiesiskajai situācijai. Pretrunīgas jurisdikcijas ir novērtētas.

Pēc kā to var atpazīt: Pierādījums ir pārskats par piemērojamajām prasībām (GDPR, valsts noteikumi, nozarei specifiski pienākumi) ar atbildīgo un pārskatīšanas datumu. Mazā uzņēmumā pietiek ar vienas lappuses sarakstu, ko pārskata reizi gadā. Jautājums piegādātājam: vai piegādātājs vai tā apakšuzņēmēji ir pakļauti jurisdikcijām, kas ļauj iestādēm piekļūt mūsu datiem, un kā ar to rīkojas?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

Prasības ir formulētas patstāvīgi un neaizstāj standarta tekstu. Saistošs ir tikai attiecīgā izdevēja oriģinālais standarts. Šis saraksts ir darba rīks, nevis atbilstības pierādījums un ne sertifikācija. Leanshift nav sertificēts pēc neviena no šiem standartiem, nav sertifikācijas institūcija un nav saistīts ar ISO, IEC, DIN, IATF, IAQG vai SAE. Šābu gadījumā ir spēkā šī saraksta vācu valodas versija.